Département de Mathématiques et Informatique **Année 1999-2000**

D.E.U.G. M.A.S.S. ou I.U.P. (en gros D.E.U.G. A 1 et 2) Algèbre

Quelques idées d'exos

Exercice 1 : Quelques calculs de limites en zéro

Déterminer si elles existent les limites en zéro des fonctions suivantes :

$$\frac{1}{x}\ln\left(\frac{\sin x}{x}\right), \qquad \frac{1}{x^2}\ln\left(\frac{\sin x}{x}\right), \qquad \frac{x(1+\cos x)-2\tan x}{2x-\sin x-\tan x}, \qquad \frac{x+\sin x}{1-\cos x}, \qquad \frac{e^x-e^{\sin x}}{x^3}.$$

Exercice 2 : L'équation de Fermat $x^2+y^2=z^2$

L'objet de cet exercice est de prouver les solutions **entières strictement positives** de l'équation :

$$x^2+y^2=z^2 \tag{E}$$

sont (à une permutation près de x et y) de la forme :

$$x=d(u^2-v^2) \qquad y=2duv \qquad z=d(u^2+v^2)$$

où d,u,v sont des entiers, les deux derniers étant premiers entre eux.

1. Commencer par vous assurer que les solutions avancées vérifient bien l'équation (E).

2. Soit d le pgcd de x,y et z. Montrer que les entiers x/d, y/d et z/d sont encore solution de (E).

À partir de maintenant on suppose que x,y et z sont premiers dans leur ensemble.

3. Montrer qu'ils le sont nécessairement deux-à-deux.

4. En déduire que deux d'entre eux sont impairs et que le troisième est nécessairement pair.

5. Montrer que x et y sont de parité distincte en procédant ainsi :

a. Vérifier que le carré d'un nombre impair est toujours congru à 1 modulo 4 et que celui d'un nombre pair est toujours congru à zéro modulo 4.

b. En raisonnant par l'absurde, c'est-à-dire en supposant que x et y sont tous deux impairs, aboutir à une contradiction.

c. Conclure.

À partir de maintenant on suppose que x impair, y pair et donc z impair.

On écrit l'équation (E) sous la forme suivante :

$$y^2=z^2-x^2=(z-x)(z+x)$$

6. En remarquant que $2x=(z+x)-(z-x)$ et que $2z=(z+x)+(z-x)$ montrer que $\mathrm{pgcd}(z+x,z-x)=2$.

On peut donc introduire $x',y',z'\in\mathbb{Z}$ tels que $y=2y'$, $z+x=2x'$ et $z-x=2z'$ si bien que ${y'}^2=x'z'$.

7. Pourquoi les entiers x' et z' sont-ils premiers entre eux ? En déduire que x' et z' sont nécessairement des carrés (indication : utiliser l'égalité ${y'}^2=x'z'$).

8. En récapitulant ce que vous avez montré, vous devez être en mesure de conclure.

Correction :

1. C'est une simple vérification. En particulier, on en déduit l'existence de solutions comme souhaitées.

À partir de maintenant $(x, y, z) \in \mathbb{N}^3$ désigne un triplet de solutions de (E) et on va montrer que nécessairement ce triplet se met sous la forme annoncée en en-tête.

2. Tout d'abord, si $d = \text{pgcd}(x, y, z)$, alors d^2 divise chacun des carrés x^2, y^2 et z^2 ; on peut donc diviser par d^2 l'égalité (E) tout en restant dans $\mathbb{Z}$: $\frac{x^2}{d^2} + \frac{y^2}{d^2} = \frac{z^2}{d^2}$, ce qui permet de dire que le triplet $(x/d, y/d, z/d)$ est encore solution de (E).

3. On suppose que les entiers x, y, z sont premiers entre eux dans leur ensemble et on veut prouver qu'ils le sont nécessairement deux-à-deux. Raisonnons par l'absurde en supposant que deux d'entre eux ne sont pas premiers entre eux ; alors ils sont divisibles par un premier p. Mais alors le carré du troisième qui est égal à la somme ou à la différence des carrés des deux premiers — car le triplet (x, y, z) est solution de (E) — est lui aussi divisible par p. Comme p est premier, p divise le carré du troisième entraîne que p divise ce dit troisième. Cela contredit le fait que x, y et z sont premiers entre eux dans leur ensemble. Nécessairement ils sont donc premiers entre eux deux-à-deux.

4. Les entiers x, y et z étant premiers deux-à-deux, au plus un d'entre eux est pair ; autrement dit, au moins deux d'entre eux sont impairs. En particulier, le carré d'au moins deux d'entre eux est impair (car le carré d'un nombre impair est lui même impair). Isolons ces deux carrés impairs, alors le troisième carré qui est égal à la somme ou à la différence des deux carrés impairs est nécessairement pair. Au moins un des carré est donc pair d'où il découle qu'au moins un des entiers x, y ou z est lui même pair. En bref, parmi les entiers x, y et z il y en a deux impairs et un pair.

5. Montrons que x et y sont de parité distincte.

a. Un nombre impair s'écrit $2k + 1$; son carré est donc égal à $4k^2 + 4k + 1$ qui est bien un entier congru à 1 modulo 4. Quant à un nombre pair, il s'écrit $2k$ donc son carré, qui vaut $4k^2$, est bien congru à zéro modulo 4.

b. Si x et y sont tous deux impairs, alors $x^2 \equiv 1 \pmod 4$ et $y^2 \equiv 1 \pmod 4$ donc $x^2 + y^2 \equiv 2 \pmod 4$. Comme $z^2 = x^2 + y^2$, on en déduit que $z^2 \equiv 2 \pmod 4$. Ceci est contradictoire puisque nous venons de montrer que le carré d'un entier est congru soit à 0 soit à 1 modulo 4.

c. L'hypothèse faite au début de la question précédente est donc fausse : les entiers x et y sont bien de parité distincte.

6. On suppose que x est impair et que y est pair. Montrons que $\text{pgcd}(z+x, z-x) = 2$. Tout d'abord, les entiers x et z étant tous les deux impairs, 2 divise bien $z+x$ et $z-x$ donc 2 divise $\text{pgcd}(z+x, z-x)$. De plus, compte tenu des égalités $2x = (z + x) - (z - x)$ et $2z = (z + x) + (z - x)$ tout diviseur commun à $z + x$ et $z - x$ est un diviseur commun à $2x$ et $2z$. Mais x et z étant premiers entre eux, on a $\text{pgcd}(2x, 2z) = 2$. En conséquence, $\text{pgcd}(z+x, z-x)$ divise 2. Cela montre que $\text{pgcd}(z+x, z-x) = 2$.

7. Comme $z + x = 2x'$ et $z - x = 2z'$ et comme $\text{pgcd}(z + x, z - x) = 2$, nécessairement x' et z' sont premiers entre eux.

Introduisons $p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ et $q_1^{\beta_1} \cdots q_s^{\beta_s}$ les décompositions primaires respectives de x' et z'. Comme x' et z' sont premiers entre eux, les premiers p_i et q_j sont deux-à-deux distincts. Par conséquent, la décomposition primaire de ${y'}^2 = x'z'$ est la suivante :

$$p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}$$

Comme ${y'}^2$ est un carré, nécessairement les exposants α_i et β_j sont tous pairs, ce qui montre que x' et z' sont tous deux des carrés.

8. Simple récapitulatif.

Exercice 3 : Histoire de changer d'air, mais non de bases !

Munissons $\mathbb{R}^3$ de sa base canonique $\mathcal{B} = \{e_1, e_2, e_3\}$ — avouez que vous êtes en présence d'un début d'exercice original, n'est-ce pas ? —. Introduisons $f \in \mathcal{L}(\mathbb{R}^3)$ dont la matrice dans la base canonique est la suivante :

$$M = \text{Mat}(f, \mathcal{B}) = \begin{pmatrix} -3 & 1 & 4 \\ 0 & 2 & 0 \\ -2 & 1 & 3 \end{pmatrix}$$

et posons $\varepsilon_1 = (1, 0, 1)$, $\varepsilon_2 = (1, 1, 1)$ et $\varepsilon_3 = (2, 0, 1)$.

1. Prouver que $\mathcal{C} = \{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$ est une base de $\mathbb{R}^3$.

2. Dresser $N = \mathrm{Mat}(f, \mathcal{C})$ la matrice de f dans la base $\mathcal{C}$.

3. Déterminer N^n pour $n \geqslant 1$.

4. En déduire l'expression de M^n pour $n \geqslant 1$.

Correction :

1. ok.

2. Notons P, la matrices des coordonnées des ε_i dans la base $\mathcal{B}$ alors :

$$P = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \qquad \Longrightarrow \qquad P^{-1} = \begin{pmatrix} -1 & -1 & 2 \\ 0 & 1 & 0 \\ 1 & 0 & -1 \end{pmatrix}$$

Avec ces notations, on a :

$$N = P^{-1}MP = P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ & 0 & -1 \end{pmatrix}$$

3. ok.

4. On en déduit que :

$$M^n = PN^nP^{-1} = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2^n & 0 \\ & 0 & (-1)^n \end{pmatrix} \begin{pmatrix} -1 & -1 & 2 \\ 0 & 1 & 0 \\ 1 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 2(-1)^n - 1 & 2^n - 1 & 2(-1)^{n+1} + 2 \\ 0 & 2^n & 0 \\ (-1)^n - 1 & 2^n - 1 & (-1)^{n+1} + 2 \end{pmatrix}$$

ceci quel que soit n.

Exercice 4 : Le résultant de deux polynômes, aperçu

Soient P et Q deux polynômes de $K[X]$ (où $K = \mathbb{R}$ ou $\mathbb{C}$) de degré p et q respectivement :

$$P(X) = a_pX^p + \cdots + a_0 \qquad \text{et} \qquad Q(X) = b_qX^q + \cdots + b_0$$

Une fois n'est pas coutume, pour $n > 0$, on note $K_n[X]$ l'ensemble des polynômes de degré **strictement** inférieur à n — au fait quelle est la dimension de cet espace — que l'on munit de la base $\mathcal{B}_n = \{X^{n-1}, X^{n-2}, \ldots, X, 1\}$. Enfin, on introduit l'application :

$$\begin{array}{rccc} \varphi : & K_q[X] \times K_p[X] & \longrightarrow & K_{p+q}[X] \\ & (U, V) & \longmapsto & UP + VQ \end{array}$$

L'espace de départ est muni de la base $\mathcal{B}_q \times \mathcal{B}_p = \{(X^{q-1}, 0), \ldots, (1, 0), (0, X^{p-1}), \ldots, (0, 1)\}$ et celui d'arrivée de la base $\mathcal{B}_{p+q}$.

1. Vérifier que φ est une application linéaire et dresser, dans les bases fixées précédemment, la matrice de l'application φ pour $p = 6$ et $q = 4$ par exemple.

On définit le **résultant** des polynômes P et Q, noté $\mathrm{res}(P, Q)$, comme étant le déterminant de cette application : $\mathrm{res}(P, Q) = \det(\varphi)$.

2. Calculer ce résultant pour $p = q = 1$ pour $p = 2$ et $Q = P'$ (poser $P(X) = aX^2 + bX + c$ dans le deuxième cas, histoire de peut-être vous interpeller).

3. Nous allons établir un certain nombre de formules liées au résultant ; dans chacun des cas avant de vous attaquer au cas général, traiter des cas particuliers avec de petites valeurs de p et q.

a. Vérifier que pour $r \in K$, on a $\mathrm{res}(X - r, Q) = Q(r)$.

b. Montrer que $\mathrm{res}(XP, Q) = Q(0)\,\mathrm{res}(P, Q)$.

c. Montrer que pour $r \in K$, on a $\mathrm{res}(P(X - r), Q(X - r)) = \mathrm{res}(P, Q)$.

d. Gr,ce aux deux questions précédentes prouver que :

$$\operatorname{res}((X-r)P,Q) = Q(r)\operatorname{res}(P,Q) \qquad \text{et} \qquad \operatorname{res}((X-r_1)\cdots(X-r_p),Q) = Q(r_1)\cdots Q(r_p)$$

les r_i et r étant des éléments de K.

4. Montrer le résultat[1] fondamental suivant : les polynômes P et Q ont une racine commune dans $\mathbb{C}$ si et seulement si $\operatorname{res}(P,Q) = 0$.

5. Confronter le résultat précédent aux exemples du début de cet exercice. Notamment, le deuxième résultant, calculé à cette occasion, ne vous rappelle-t-il pas, à un coefficient près, un certain réel (ou complexe) associé au polynôme $aX^2 + bX + c$.

6. Considérons maintenant le résultant de P et Q comme un déterminant à coefficients dans $K[X]$, plutôt que dans K.

a. Pour $1 \leqslant i \leqslant p+q$, on note L_i la i-ème ligne du déterminant définissant $\operatorname{res}(P,Q)$; effectuer l'opération sur les lignes indiquée ci-dessous :

$$L_{p+q} \leftarrow X^{p+q-1}L_1 + X^{p+q-2}L_2 + \cdots + XL_{p+q-1} + L_{p+q}$$

et montrer que $\operatorname{res}(P,Q)$ peut se définir comme un déterminant à coefficients dans $K[X]$ tous les coefficients étant constants sauf ceux de la dernière ligne qui sont de la forme X^iP ou X^jQ avec $0 \leqslant i < q$ et $0 \leqslant j < p$ (conseil d'ami : effectuer tout d'abord cette opération pour deux valeurs de p et q petites, par exemple $p = 6$ et $q = 4$).

b. En utilisant la nouvelle expression du résultant que vous venez de mettre en évidence, prouver qu'il existe $(U,V) \in K_q[X] \times K_p[X]$ tel que $\operatorname{res}(P,Q) = UP + VQ$.

c. Retrouver le fait que si P et Q ont une racine commune dans $\mathbb{C}$ alors leur résultant est nul.

Correction :

1. Pour fixer les idées, on a :

$$\operatorname{res}(a_6X^6 + \cdots + a_0, b_4X^4 + \cdots + b_0) = \begin{vmatrix} a_6 & 0 & 0 & 0 & b_4 & 0 & 0 & 0 & 0 & 0 \\ a_5 & a_6 & 0 & 0 & b_3 & b_4 & 0 & 0 & 0 & 0 \\ a_4 & a_5 & a_6 & 0 & b_2 & b_3 & b_4 & 0 & 0 & 0 \\ a_3 & a_4 & a_5 & a_6 & b_1 & b_2 & b_3 & b_4 & 0 & 0 \\ a_2 & a_3 & a_4 & a_5 & b_0 & b_1 & b_2 & b_3 & b_4 & 0 \\ a_1 & a_2 & a_3 & a_4 & 0 & b_0 & b_1 & b_2 & b_3 & b_4 \\ a_0 & a_1 & a_2 & a_3 & 0 & 0 & b_0 & b_1 & b_2 & b_3 \\ 0 & a_0 & a_1 & a_2 & 0 & 0 & 0 & b_0 & b_1 & b_2 \\ 0 & 0 & a_0 & a_1 & 0 & 0 & 0 & 0 & b_0 & b_1 \\ 0 & 0 & 0 & a_0 & 0 & 0 & 0 & 0 & 0 & b_0 \end{vmatrix}$$

(c'est donc une matrice carrée $(p+q) \times (p+q)$)

2. Pour $p = q = 1$, on trouve $\operatorname{res}(P,Q) = a_1b_0 - a_0b_1$; le deuxième exemple donne :

$$\operatorname{res}(aX^2 + bX + c, 2aX + b) = -a(b^2 - 4ac)$$

qui, à une constante près, n'est rien d'autre que l'ultra-classique discriminant de aX^2+bX+c souvent noté Δ.

3. Quelques propriétés.

a. Il suffit de développer par rapport à la dernière colonne.

b. Il suffit de développer par rapport à la dernière ligne.

[1] J'attire votre attention sur le fait que ce test est complètement effectif (i.e. programmable en machines). Sachez de plus que le résultant est un déterminant loin d'être quelconque ; d'ailleurs, il existe des algorithmes spécifiques (et assez sophistiqués) permettant de calculer un résultant efficacement. Autrement dit, tout système de calcul formel digne de ce nom n'utilise jamais la fonction *déterminant* — si cette dernière existe — pour calculer un résultant.

c. Écrire le premier résultant dans les bases constituées d'éléments de la forme $(X-r)^i$.

d. D'après ce qui précède :

$$\begin{aligned}\operatorname{res}((X-r)P(X),Q(X)) &= \operatorname{res}(XP(X+r),Q(X+r))\\ &= Q(r)\operatorname{res}(P(X+r),Q(X+r)) = Q(r)\operatorname{res}(P(X),Q(X))\end{aligned}$$

La deuxième formule découle directement de la dernière.

4. Évident compte tenu des formules précédentes.

5. On retrouve le fait que le polynôme aX^2+bX+c admet une racine double quand $\Delta = 0$.

6. S'y va !

a. Après la manipulation indiquées, la dernière ligne du déterminant $\operatorname{res}(P,Q)$ vaut :

$$\begin{bmatrix} X^{q-1}P & X^{q-2}P & \cdots & XP & P & X^{p-1}Q & X^{p-2}Q & \cdots & XQ & Q\end{bmatrix}$$

b. Il suffit de développer par rapport à la dernière ligne.

c. ok.

Exercice 5 : Le résultant est le bon résultat (bof !)

Soient $P(X) = X^3+X+1$ et $Q(X) = X^2+1$ deux polynômes de $\mathbb{C}[X]$ et soit φ l'application linéaire définie par :

$$\varphi \;:\; \begin{array}{ccc} \mathbb{C}_2[X]\times\mathbb{C}_3[X] & \longrightarrow & \mathbb{C}_5[X] \\ (U,V) & \longmapsto & UP+VQ \end{array}$$

où pour $n \geqslant 1$, la notation $\mathbb{C}_n[X]$ désigne l'espace vectoriel des polynômes de degré **strictement** inférieur à n.

1. Dresser la matrice de φ en choisissant $\mathcal{B} = \{(X,0),(1,0),(0,X^2),(0,X),(0,1)\}$ comme base au départ et $\mathcal{C} = \{X^4,X^3,X^2,X,1\}$ comme base à l'arrivée.

2. Calculer $\operatorname{res}(P,Q)$ qui, je vous le rappelle, n'est rien d'autre que le déterminant de φ.

Correction :

1. La matrice trouvée est :

$$\operatorname{Mat}(\varphi,\mathcal{B},\mathcal{C}) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0\\ 0 & 1 & 0 & 1 & 0\\ 1 & 0 & 1 & 0 & 1\\ 1 & 1 & 0 & 1 & 0\\ 0 & 1 & 0 & 0 & 1\end{pmatrix}$$

2. Son déterminant est 1.